GLASSWALL

Glasswall Email Security

Email is a popular vehicle for social engineering attacks and other threats - what employee wouldn't open an attachment that appears to be from their CEO?

Make sure only safe email attachments enter and exit your organization.
With Glasswall Email Security, every attachment is disarmed of potential threats and delivered instantly

Key benefits

- ✓ Always-on SaaS solution with multi-region support and failover for uninterrupted mail flow
- ✓ Give users the freedom to open any attachment
- ✓ Deliver mail to desktops and devices without delay
- ✓ Disarm and rebuild attachments with perfect visual content layer integrity
- ✓ Flexible, scalable processing for any file volume
- ✓ Protection without the delay of identifying malware 'Patient Zero'
- ✓ Defeat advanced malware that are 'sandbox-aware'

Key features

- Microsoft Office 365 & Exchange Online, Google Workspace and easy integration with any locally installed or cloud-based SMTP servers
- Support for all key business file formats including Binary Office, Open XML Office, PDF, PNG, JPEG, BMP, TIF. GIF, EMF, WMF, MP3, WAV, MP4 and more
- Archive support for Zip, Tar, GZip, 7Zip and Rar formats
- Unsupported file types can be allowed or disallowed for select senders and receivers by policy
- Multi-region data sovereignty support
- Role-based administration
- Easy user-defined risk policy management

Use cases

Enterprise-scale business email threat removal

Supply chain security

Secure email attachments

How it works

Glasswall Email Security uses the patented Glasswall CDR Platform to inspect, clean and rebuild email file attachments to their known good state in real-time–proactively protecting your organization against the most persistent and complex file-based threats.